

BOX PCT

ATTORNEY'S DOCKET NO: 82231

U.S. DEPARTMENT OF COMMERCE, PATENT AND TRADEMARK OFFICE		DATE: March 3, 2000 (03.03.2000)
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371		U.S. APPL. N. NO. (if known): Not Yet Assigned
INTERNATIONAL APPLICATION NO.: PCT/SG99/00086	INTERNATIONAL FILING DATE: 21 August 1999 (21.08.99)	PRIORITY DATE CLAIMED: 21 August 1999 (21.08.99)
TITLE OF INVENTION: LEGITIMACY PROTECTION OF ELECTRONIC DOCUMENT AND A PRINTED COPY THEREOF		
APPLICANT(S) FOR DO/EO/US: Jiankang WU, Qibin SUN, and Huijie DENG		

Applicant hereby submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

- ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
- ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
- ☒ This express request to begin national examination procedures (35 USC 371(f)) at any time rather than delay examination until the expiration of the time limit set in 35 USC 371(b) and PCT Articles 22 and 39(1)
- ☐ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date
- ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2)):
 - ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
 - ☒ has been transmitted by the International Bureau.
 - ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
- ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
- ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
 - ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
 - ☐ have been transmitted by the International Bureau.
 - ☐ have not been made; however, the time limit for making such amendments has NOT expired.
 - ☒ have not been made and will not be made.
- ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
- ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
- ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

ITEMS 11. TO 16. BELOW CONCERN OTHER DOCUMENT(S) OR INFORMATION INCLUDED:

- ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
- ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
- ☐ A **FIRST** preliminary amendment.
☐ A **SECOND** or **SUBSEQUENT** preliminary amendment
- ☐ A substitute specification.
- ☒ A change of power of attorney and/or address letter.
- ☒ TRANSMITTAL FORM; FEE CALCULATION; PCT APPLICATION CONSISTING OF 68 PAGES INCLUDING, 42 PAGES TEXTUAL SPECIFICATION, 20 PAGES OF 95 CLAIMS; 1 PAGE ABSTRACT; 5 SHEETS DRAWINGS (9 FIGURES); EXECUTED INVENTOR'S DECLARATION; ASSIGNMENT AND RECORDATION COVER SHEET; PCT REQUEST FORM PCT/RO/101; AND PCT FORM PCT/RO/105.

ATTORNEY'S DOCKET NO: 82231

U.S. APPLICATION NO. (if known) <div style="font-size: 2em; font-weight: bold;">09/486940</div>	INTERNATIONAL APPLICATION NO. PCT/SG99/00086	DATE: March 3, 2000 (03.03.2000)
---	---	-----------------------------------

17. <u>x</u> The following fees are submitted: Basic National Fee (37 CFR 1.492(a)(1)-(5): Search Report has been prepared by the EPO or JPO:.....\$840.00 International preliminary examination fee paid to USPTO (37 CFR 1.482).....\$670.00 No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)).....\$760.00 Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO.....\$970.00 International preliminary examination fee (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4).....\$ 96.00 <div style="text-align: right;">ENTER APPROPRIATE BASIC FEE AMOUNT =</div>	<u>CALCULATIONS</u>	<u>PTO USE ONLY</u>
<div style="text-align: right;">\$ 840.00</div>		

Surcharge of \$130.00 for furnishing the oath or declaration later than <u> 20 </u> <u> 30 </u> months from the earliest claimed priority date (37 CFR 1.492(e)).	\$	
---	----	--

CLAIMS	NO. FILED	NO. EXTRA	RATE		
TOTAL	95 -20=	75	X \$ 18.00	\$	1,350.00
INDEPENDENT	10 - 3=	7	X \$ 78.00	\$	546.00
Multiple dependent claims(s) (if applicable)			+ \$260.00	\$	0.00
TOTAL OF ABOVE CALCULATIONS =				\$	2,736.00
Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28).				\$	0.00
SUBTOTAL =				\$	2,736.00
Processing fee of \$130.00 for furnishing the English translation later than <u> 20 </u> <u> 30 </u> months from the earliest claimed priority date (37 CFR 1.492(f)).				\$	0.00
TOTAL NATIONAL FEE =				\$	2,736.00
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). <div style="text-align: right;">\$40.00 per property +</div>				\$	40.00
TOTAL FEES ENCLOSED =				\$	2,776.00
				Amount to be: refunded <hr style="width: 100px; border: 0; border-top: 1px solid black;"/> charged	\$ <hr style="width: 100px; border: 0; border-top: 1px solid black;"/> \$ <hr style="width: 100px; border: 0; border-top: 1px solid black;"/>

U.S. APPLICATION NO. (if known) 09/486940	INTERNATIONAL APPLICATION NO. PCT/SG99/00086	DATE: March 3, 2000 (03.03.2000)
--	--	----------------------------------

a. ☒ Two checks in the amount of 2,776.00 to cover the above fees, are enclosed.

b. ☐ Please charge my Deposit Account No. 14-0112 in the amount of \$_____ to cover the above fees.

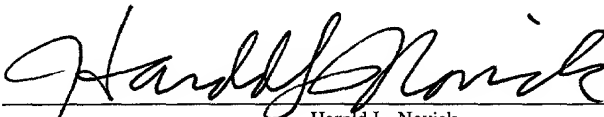
c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 14-0112.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed to request that the application be restored to pending status.

Send All Correspondence To:

Harold L. Novick
NATH & ASSOCIATES
1030 Fifteenth Street, N.W.
Sixth Floor
Washington, D.C. 20005

(202) 775-8383 (phone)
(202) 775-8396 (fax)



Harold L. Novick
Registration Number 26,011

Rev. 02/98

5 The invention relates to secure electronic and printed documents and, more particularly, to a method and apparatus for providing integrated legitimacy protection of electronic and printed documents.

10 In daily business and personal life, electronic and paper versions of a document are
equally important and are important, ubiquitous items, especially in view of the
proliferation of the Internet and like networks. Despite this, conventional approaches
of protecting the legitimacy of one form of the document have ignored protection of
the other form of the document. A number of conventional methods and systems are
15 described below.

U.S. Patent Nos. 4,981,370 (issued to Dziwit et al. on 1 January 1991), 5,031,214 (issued to Dziwit et al. on 9 July 1991), 5,163,091 (issued to Graziano, et al on 10 November 1992), and 5,191,613 (issued to Graziano, et al on 2 March 1993) describe contract (or single signer document) signing processes, addressing the problems of electronic contract signing: security, tangibility, reliability, authentication, longevity and validity. The apparatus described in these patents produces a final authenticated document using computerized techniques. The document is stated to satisfy the legal document authentication and authenticity requirements traditionally associated with printed documents. The document authentication process is activated as part of a program that verifies the identicalness of the document at the transmitting and receiving station through a high speed comparison and locks in the document so that modifications cannot occur. The process then awaits authentication handshakes from the two end points. Once the identities of the signatories of the document are verified, the document authentication apparatus prompts the parties to authenticate the document by appending an electronic signature thereto. The actual "signing" or

Variable	Mean	SD	Min	Max
Age	34.5	10.2	18	65
Gender	0.5	0.5	0	1
Marital status	0.6	0.5	0	1
Education	12.5	1.5	9	16
Income	1500	500	500	3000
Health status	0.8	0.2	0	1
Smoking status	0.3	0.5	0	1
Alcohol consumption	0.2	0.4	0	1
Exercise frequency	0.5	0.5	0	1
Stress level	0.7	0.3	0	1
Sleep quality	0.6	0.4	0	1
Work satisfaction	0.5	0.5	0	1
Life satisfaction	0.6	0.4	0	1
Overall health	0.7	0.3	0	1
Depression score	0.2	0.4	0	1
Anxiety score	0.3	0.5	0	1
Stress score	0.4	0.6	0	1
Sleep score	0.5	0.5	0	1
Work score	0.6	0.4	0	1
Life score	0.7	0.3	0	1
Health score	0.8	0.2	0	1
Smoking score	0.3	0.5	0	1
Alcohol score	0.2	0.4	0	1
Exercise score	0.5	0.5	0	1
Stress score	0.7	0.3	0	1
Sleep score	0.6	0.4	0	1
Work score	0.5	0.5	0	1
Life score	0.6	0.4	0	1
Health score	0.7	0.3	0	1
Depression score	0.2	0.4	0	1
Anxiety score	0.3	0.5	0	1
Stress score	0.4	0.6	0	1
Sleep score	0.5	0.5	0	1
Work score	0.6	0.4	0	1
Life score	0.7	0.3	0	1
Health score	0.8	0.2	0	1
Smoking score	0.3	0.5	0	1
Alcohol score	0.2	0.4	0	1
Exercise score	0.5	0.5	0	1
Stress score	0.7	0.3	0	1
Sleep score	0.6	0.4	0	1
Work score	0.5	0.5	0	1
Life score	0.6	0.4	0	1
Health score	0.7	0.3	0	1
Depression score	0.2	0.4	0	1
Anxiety score	0.3	0.5	0	1
Stress score	0.4	0.6	0	1
Sleep score	0.5	0.5	0	1
Work score	0.6	0.4	0	1
Life score	0.7	0.3	0	1
Health score	0.8	0.2	0	1
Smoking score	0.3	0.5	0	1
Alcohol score	0.2	0.4	0	1
Exercise score	0.5	0.5	0	1
Stress score	0.7	0.3	0	1
Sleep score	0.6	0.4	0	1
Work score	0.5	0.5	0	1
Life score	0.6	0.4	0	1
Health score	0.7	0.3	0	1
Depression score	0.2	0.4	0	1
Anxiety score	0.3	0.5	0	1
Stress score	0.4	0.6	0	1
Sleep score	0.5	0.5	0	1
Work score	0.6	0.4	0	1
Life score	0.7	0.3	0	1
Health score	0.8	0.2	0	1
Smoking score	0.3	0.5	0	1
Alcohol score	0.2	0.4	0	1
Exercise score	0.5	0.5	0	1
Stress score	0.7	0.3	0	1
Sleep score	0.6	0.4	0	1
Work score	0.5	0.5	0	1
Life score	0.6	0.4	0	1
Health score	0.7	0.3	0	1
Depression score	0.2	0.4	0	1
Anxiety score	0.3	0.5	0	1
Stress score	0.4	0.6	0	1
Sleep score	0.5	0.5	0	1
Work score	0.6	0.4	0	1
Life score	0.7	0.3	0	1
Health score	0.8	0.2	0	1
Smoking score	0.3	0.5	0	1
Alcohol score	0.2	0.4	0	1
Exercise score	0.5	0.5	0	1
Stress score	0.7	0.3	0	1
Sleep				

authenticating of the electronic document can be implemented as an additional password step utilizing a personnel identity validation apparatus. Therefore, two levels of password protection can be used such that there exists a separate "document authenticating password". The more sophisticated the system is the more assured a court can be that a document's authentication is valid. In this manner, no paper document version of the electronic contract need be produced. The traditional elements of a paper contract are all present in electronic form in the computer system.

Additional capabilities are obtained since this is a knowledge-based computer system and this can automate much of the document creation and authentication process. In particular, the creation of a multi-party document, such as a contract, entails a significant amount of interaction among the contracting parties. This is especially efficient in the arena of Electronic Document Interchange (EDI), where standard form messages are exchanged between the parties to order and invoice goods.

Thus, these four patents deal with electronic contract negotiation and signing process. However, the disclosure of these documents fails to address an integrated solution for both electronic and printed documents and on ways to make a document tangible and acceptable to people.

U.S. Patent No. 5,742,685 (issued to Berson, et. al. on 21 April 1998) describes a method for verifying an identification card and recording verification of the same. A person whom the identification card identifies is scanned to produce a digital signal associated with some text message, which is compressed, encrypted, coded as a 2-D barcode, and printed on the backside of the identification card. To validate the card, the coded message is scanned, decoded, and decrypted, expanded, and displayed. Authentication can be carried out by comparing the displayed image and text with the image and text printed on the card.

Similarly, Huttinger, Stephan, "Online Ticket" Computer Graphik, Vol. 11, pp. 9-10, Jan. 1999 describes an online ticket that is delivered to a customer, which is selected and paid via the Internet. On the ticket, a 2-D barcode is provided representing the

data of the tickets and signature. A digital signature technique is used to prove the authenticity of the ticket.

U.S. Patent No. 4,853,961 (issued to Pastor on 1 August 1989) describes a system for authenticating a document, including a device having a decryption key. Upon application to information provided by a user, the system reveals not only a plain text message indicating the source of the authentication but also provides the decryption key for use with the information provided by the mailer. Similarly, US Patent No. 5,388,158 (issued to Berson on 7 February 1995) describes a secure document and a method and an apparatus for producing and authenticating the same. A document is scanned to produce a digital signal, which is compressed, encrypted, and coded as a two-dimensional barcode or like form of coding. The barcode is incorporated into a label affixed to the document. A signal representing the image is encrypted using a public key encryption system, and the key is downloaded from a center. To facilitate authentication, the corresponding decryption key is encrypted with another key and incorporated on the card. To validate the document, the coded signal is scanned from the label, decoded, decrypted, expanded and displayed. The card may then be authenticated by comparison of the displayed representation of the image and the document.

U.S. Patent No. 5,157,726 (issued to Merkle, et. al. on 20 October 1992) describes a system for authenticating a hard copy of an original document. At the sender's station, the original document and an identification (ID) card are inserted into a special copying machine. The machine digitizes the document text to produce a digital signature, which incorporates unique information from the sender's ID card. This machine produces a hard copy of the document, to which is added the digital signature. The sender retains the original, but forwards the copy to the recipient or receiver. The receiver inserts the received copy into the machine at his location, which digitizes and processes the document text and signature and indicates whether the digital signature is valid.

- U.S. Patent No. 5,710,886 (issued to Christensen, et. al. on 20 January 1998) describes a method for distributing, generating, and redeeming discount coupons, rebate or gift certificates. The method tracks each coupon using a consumer ID number printed on the coupon. Coupons may be distributed electronically, for example, in the form of a diskette or CD-ROM software. Software on the diskette or CD-ROM may prompt a consumer to call a 1-800 number for a validation number or code. During the phone call, telemarketing personnel request consumer demographic and or identification information, which can be entered into a centralized database. Once the software is validated, a consumer may print out selected coupons. Each coupon can be printed only a limited number of times. Each coupon can also be imprinted with a consumer ID number, preferably in the form of a bar code. The patent states that "the use of a consumer ID number on the coupon may reduce or prevent the fraudulent copying and redemption of coupons".
- U.S. Patent Nos. 5,374,976 (issued to Spannenburg on 20 December 1994), 5,823,576 (issued to Lambert on 20 October 1998) and 5,018,767 (issued to Wicker on 28 May 1991) describe methods for protecting paper documents against photocopying. These methods use a high resolution printing machine (e.g., 600 dpi), to print a document with embedded patterns. These embedded patterns are not visible on the original document. After being photocopied by an ordinary photocopier, which has a lower resolution (e.g. 300 dpi) the patterns become visible.

The above techniques have a number of disadvantages. Firstly, the techniques for electronic document authentication are not user-friendly. In other words, the techniques do not make the electronic document tangible or easily comprehensible to users. An encryption key or 2-D barcode is not directly readable by users, and the users do not know whether the document or item is authorized and by whom the document is authorized. Secondly, technologies are not known to exist that provide an integrated solution for both electronic and printed document. This is critical for mission-critical applications, either for business or daily life. With an integrated solution, the benefit of high-speed delivery via the Internet and an Intranet can be enjoyed, while keeping the convenience and tangibility of a paper document. Thirdly,

the protection provided by these techniques is not personalized. This is also important for legal and business document, where each person would be interested in protecting or being responsible for the content of his/her part.

5 U.S. Patent Nos. 5,742,685 (issued to Berson, et. al. on 21 April 1998), 4,853,961 (issued to Pastor on 1 August 1989) and 5,388,158 (issued to Berson on 7 February 1995) disclose methods or systems for protecting electronic or paper document using cryptographic technique. However, these systems have a number of disadvantages including:

- 10 1) The methods or systems only provide a solution for an electronic or paper document only;
- 2) The methods or systems are based on cryptographic techniques, which are secure for an electronic document, but are not tangible and convenient to users in many applications. A paper document is still
- 15 preferable for many applications and preferred by many people;
- 3) The protection is not personalized, even true for documents with multiple signers; and
- 4) There is no total solution/product/service for authentication and delivery.

20 Thus, a need clearly exists for a method of protecting the legitimacy of both electronic and printed versions of a document overcoming, or at least ameliorating, one or more of the foregoing disadvantages.

SUMMARY OF THE INVENTION

25 The aspects of the invention seek to provide an integrated method of protecting the legitimacy of electronic document and a corresponding printed version. This is implemented by user-friendly e-seals. The protection is personalized using a personal e-seal. Documents with multiple signers can be effectively and efficiently protected and verified.

30

In accordance with a first aspect of the invention, there is disclosed an electronic document for reproduction of a corresponding printed document capable of having the

legitimacy of the electronic document protected, the printed document being a printed version of the electronic document, the electronic document including: content of an original document in electronic form; a content digest for the content the original document in electronic form; an electronic seal or e-seal for authenticating the original document in electronic form, the e-seal including a visible seal of an authority and the content digest embedded in the visible seal; an optically sensitive or sensible component added to the authenticated document for printing using a trusted printing process, the optically sensitive or sensible component containing information for indicating copying or modification of the printed document in a copy or modified version of the printed document.

In accordance with a second aspect of the invention, there is disclosed a printed document reproduced from an electronic document capable of having the legitimacy of the printed document protected, the printed document being a printed version of the electronic document, the printed document including: rendered content of an original document; an electronic seal or e-seal for authenticating the original document rendered in the printed document, the e-seal including a visible seal of an authority and a content digest for the content of the original document embedded in the visible seal; an optically sensitive or sensible component rendered in the authenticated document using a trusted printing process, the optically sensitive or sensible component containing information for indicating copying or modification of the printed document in a copy or modified version of the printed document.

In accordance with a third aspect of the invention, there is disclosed a method of protecting the legitimacy of an electronic document and a corresponding printed document, the printed document being a printed version of the electronic document, the method including the steps of: generating a content digest for an original document in electronic form; authenticating the original document in electronic form using an electronic seal or e-seal, the e-seal including a visible seal of an authority and the content digest embedded in the visible seal; adding an optically sensitive or sensible component to the authenticated document for printing using a trusted printing process, the optically sensitive or sensible component containing information for

indicating copying or modification of the printed document in a copy or modified version of the printed document.

In accordance with a fourth aspect of the invention, there is disclosed an apparatus for protecting the legitimacy of an electronic document and a corresponding printed document, the printed document being a printed version of the electronic document, the apparatus including: means for generating a content digest for an original document in electronic form; means for authenticating the original document in electronic form using an electronic seal or e-seal, the e-seal including a visible seal of an authority and the content digest embedded in the visible seal; means for adding an optically sensitive or sensible component to the authenticated document for printing using a trusted printing process, the optically sensitive or sensible component containing information for indicating copying or modification of the printed document in a copy or modified version of the printed document.

In accordance with a fifth aspect of the invention, there is disclosed a computer program product having a computer usable medium having a computer readable program code means embodied therein for protecting the legitimacy of an electronic document and a corresponding printed document, the printed document being a printed version of the electronic document, the computer program product including: computer readable program code means for generating a content digest for an original document in electronic form; computer readable program code means for authenticating the original document in electronic form using an electronic seal or e-seal, the e-seal including a visible seal of an authority and the content digest embedded in the visible seal; computer readable program code means for adding an optically sensitive or sensible component to the authenticated document for printing using a trusted printing process, the optically sensitive or sensible component containing information for indicating copying or modification of the printed document in a copy or modified version of the printed document.

In accordance with a sixth aspect of the invention, there is disclosed a system utilising a network for protecting the legitimacy of an electronic document and a

5

15

20

25

30

5

15

30

5
10

BRIEF DESCRIPTION OF THE DRAWINGS

15

20

Fig. 2 is a block diagram illustrating a content definition scheme for documents with multiple signers in accordance with the first embodiment of the invention;

25

30

Fig. 5 is a block diagram illustrating a process of electronic document authorization using an e-seal in accordance with the first embodiment of the invention;

Fig. 6 is a block diagram illustrating a verification process for an electronic document in accordance with the first embodiment of the invention;

5 Fig. 7 is a block diagram illustrating a printing process for converting an electronic document into a printed version in accordance with the first embodiment of the invention;

Fig. 8 is a block diagram illustrating a verification process for paper document in
10 accordance with the first embodiment of the invention; and

Fig. 9 is a diagram symbolically illustrating a service center for certification/notarisation in accordance with the embodiments of the invention.

15 DETAILED DESCRIPTION

An electronic document and a printed document capable of having their legitimacy protected, and a method, an apparatus, a computer program product and a system for protecting the legitimacy of electronic and printed documents are described. In the following description, numerous details are set forth including specific encryption techniques, water marking techniques, content digesting methods and the like, for example. It will be apparent to one skilled in the art, however, that the present invention may be practiced without these specific details. In other instances, well-known features are not described in detail so as not to obscure the present invention.

25 For ease of description, the embodiments of the invention are each described or referred to as a “system”. Components of the system are described as modules. A module, and in particular the module’s functionality, can be implemented in either hardware or software. In the software sense, a module is a process, program, or portion thereof, that usually performs a particular function or related functions. In the
30 hardware sense, a module is a functional hardware unit designed for use with other components or modules. For example, a module may be implemented using discrete electronic components, or it can form a portion of an entire electronic circuit such as

an Application Specific Integrated Circuit (ASIC). Numerous other possibilities exist. Those skilled in the art will appreciate that the system can also be implemented as a combination of hardware and software modules.

- 5 For convenience and ease of reference, the description includes the following sections:

- 10 4. Product/Services

1. Overview of System

The embodiments of the invention provide an integrated document legitimacy protection system, including four products/services providing speedy delivery of trusted electronic and paper documents via the Internet and/or an Intranet, and certification/notarization services. The embodiments provide methods and products for legitimacy protection of an electronic and printed documents using an electronic seal, or “e-seal”. The e-seal is a visual representation of a person’s authentication of the document, and includes three major components: 1) a visible seal providing a visual identity of the person, which can be an image containing a logo, a real seal, a signature of the person, or a combination of them (with an e-seal people immediately know who authorized the document); 2) a watermark, embedded into the seal images to protect the integrity of the document and the watermarking information contains digest of the document content protected by cryptographic operations. Any modification of document content creates inconsistency between the content and the e-seal. To provide integrated protection for both electronic and paper documents, a novel digest derivation algorithm is utilised, which generates a similar digest for electronic and paper versions of a document; 3) an optically sensitive component is added to the printed document on the fly by a special printing method, controlled by a trusted party, to verify that the document’s legitimacy before printing. The optical sensitive component protects the original printed document from possible forgeries, such as cut-and-paste and duplication by photocopying and rescanning. With the

5

10

15

20

30

2. The E-seal and E-seal Components

Again, an electronic seal or e-seal in accordance with the embodiments of the invention includes a visible image identifying a person's authentication of a document. The e-seal represents effective and efficient protection regarding the integrity of the document. Figs. 1A-1C illustrate an example of an e-seal in accordance with the embodiments of the invention. Each e-seal preferably has three components: a visible or seal image, a watermark containing a digest of the content of a document, and an optically sensitive or sensible component.

Fig. 1A shows an e-seal 110, which can be attached to, or incorporated in, an electronic document (not shown). For ease of illustration, the e-seal 110 is depicted in a black-line rectangle. The e-seal 110 includes an image of a person's signature 110A (Jiankang Wu) acting as a visual identifier of the signer of the document. The visible seal 110A is kept in digital image format. Other visible images 110A besides a person's signature may be practised without departing from the scope and spirit of the invention. For example, the visible image 110A may be a document header, a logo, an image of a person's face, a graphical symbol, and the like. Numerous possibilities exist which will be apparent to those skilled in the art in view of the disclosure herein. Still further, the visible image 110A is preferably watermarked with information about the owner of the visible seal 110A to protect the ownership of the visible seal 110A. The e-seal 110 also includes a watermark 110B appearing as a noise-like strip under the image of the signature 110A. The watermark 110B conveys the digest of the document's content (i.e., the information contained in the document including text, images, and the like) to protect the integrity of the document. The digest of content is described in greater detail hereinafter.

Fig. 1B illustrates a corresponding e-seal 120 rendered on a printed document (not shown) and again depicted within a black-line rectangular box. The e-seal 120 includes a visible seal 120A and a watermark 120B containing the digest of the document's content. A grey, rectangular optical sensitive or sensitive component 120C is added right under the watermark strip in the printed document when rendered. This is done prior to rendering of the drawing using a trusted rendering process.

Optionally, a serial number (i.e., 99072002) is added in the component area 120C to identify the printed document. The optically sensitive or sensible component 120 contains information for indicating copying or modification of the printed document in a copy or modified version of the printed document. Fig. 1C is a depiction of an e-seal 130 in a photocopy of the original printed document containing the e-seal 120 of Fig. 1B. In Fig. 1C, the photocopied e-seal 120 has changed appearance so that an imperceptible portion of the optically sensitive component 120 is now perceptible (i.e., the signature of Jiankang Wu) in the photocopied e-seal 130.

10 2.1 Visible E-seal

In the embodiments of the invention, a visible seal can be viewed as a user-friendly interface and a visual identity of an authority. Huttinger, Stephan, "Online Ticket", Computer Graphik, Vol. 11, pp 9-10, January 1999 discloses a two-dimensional (2-D) bar code for authorization of document, which is an easily detectable code of encrypted information. A bar code is a printed binary code, which can be detected by a bar code reader with a very low error rate, but is not readable by a human being. That is, with a bar code on a document, who the document is authorised by is not known, and a user cannot determine if the bar code is a valid one or not without a testing device.

20 An authority, either an organisation or individual, often has a unique "seal", which can be a logo, a signature, or the like. The image of the foregoing is the visible seal component of the e-seal. To protect the ownership of the e-seal, an invisible watermark is preferably embedded into the seal image. The invisible watermark information may include, but is not limited to, the name of the owner and the date of generation of the seal. Other information may be included in the seal image. If the watermarking process is not invertible, another person cannot pretend to be the owner. Image watermarking for copyright protection is discussed in Cox, Ingemar J., and Miller, Matt L., "A Review of Watermarking and the Importance of Perceptual Modeling", Proc. Of Electronic Imaging '97, February 1997.

A seal image can be locked by the owner using, for example encryption, and stored in a secure place. The owner unlocks the seal image and uses the seal image to sign a

document. Access to and unlocking the seal image can be done using a password, a smart card, or biometrics.

2.2 Watermarking a Digest of Content

5 Seals and signatures on a paper document can provide evidence of the legitimacy of the document, because the originality of the seal and the signature on the paper can be verified simply by visual inspection. For an electronic document, protection of the content of the document from unauthorised or illegal changes is mainly realized by a watermark, which is embedded into the e-seal image(s). The watermark information
10 contains a “digest” of the document content. There are two major types of applications requiring document legitimacy protection: The first type of applications are those where documents are issued by trusted authorities. Examples include government gazettes and tickets, where the authorities or their agencies carry out the legitimacy verification. In terms of information security, the authority / key-issuer and
15 verifier share security keys.

The second type of applications are those where documents are transferred among multiple parties. Examples include electronic legal document, and official documents in government or large companies. There may be multiple persons initiating the
20 document and a need exists for a trusted third party issuing keys.

The word “key” includes a piece or set of information, with which a message or device can be transferred from one state to another by a specific function. For example, a security key can be used to encrypt a message. Alternatively, a set of
25 eigenfaces being a face image mapped into a small dimension feature vector can be used. Still further, watermark information can be embedded into an image with a secret address. In the above three examples, a security key, eigenfaces and an embedding address can be all referred to as “keys” and are merely illustrative. Numerous other possible key exist and will be appreciated by those skilled in the art.

30

2.2.1 Content of a Document

The embodiments of the invention seek to protect document content from possible tampering and/or unauthorised use. Therefore, defining the document content in the protection process is of significant importance, especially for those documents signed by multiple persons.

5

Basically, the content of the document refers to all information contained in the document at the time of signing (i.e. applying an e-seal to the document), including layout and format. For a document with multiple signers, the content is defined as content with respect to a particular signer. A first example is where the contract is signed by two parties. In a first round, both parties sign a plain document, being one of two copies of a contract. The contract content is the content of the document. In a second round, each party signs the other document that is already signed by the other party. In this case, the content of the document includes the signature the other party. Fig. 2 shows a second example illustrating the idea of content definition with respect to a particular signer of the document using a three signer example. A document 200 containing initial content 222 is initiated and signed by a first person, and sent to a second person. The second person signs the document and sends it to a third person. For the first person, the content 222 of the document 200 seen is the whole information contained in the original document, shown as box 222. When the second person signs the document 200, the document content 220 with respect to that person should include the content 222 of the original document 200, the first person's signature 224 and the second person's addition 226 (such as comments) to the document. To the third person, the content 230 of the document 200 includes the original document 222, the signatures of the first person (224) and second person, addition to the document by the second person 226 and the third person 236. Note that, the signature of the person is implemented as e-seal. This can be formally written as:

$$C_n = \sum_{i=1}^n (S_{i-1} + \delta_i) + C_0$$

where C_n is the content of the document at the time of signing by the n^{th} person, S_{i-1} is the signature of the previous signer, the first signing person has a sequence number of 0, and δ_i is the addition to the document by i^{th} signing person.

- 5 In the embodiments of the invention, the digest of the document content is embedded into the e-seal of the person when the document is signed by that person.

There is redundancy if the digest of the document content includes the original document again when the next person signs the document. The redundancy occurs because the digest of the original document content exists in all e-seals of all signing persons.

For reasons of consistency, when a person signs a document, the person verifies the legitimacy of that document against all existing signatures from the first to the last.

- 15 An alternative method is to just embed the digest of the last e-seal and the person's addition to the document when a person signs the document. That is, the content of the first signer is C_0 , the content of the subsequent signers i are: $S_{i-1} + \delta_i$. This is secure and simpler for the following reasons:

- 1) The last e-seal carries the digest of the content of the document at the time of signing and, therefore, all e-seals form a protection chain. Breaking any part of the chain results in unsuccessful authentication.

- 2) The digest of content for the i^{th} signer can be written as:

$$D_i = d(S_{i-1} + \delta_i) = d(S_{i-1}^{image} + d(S_{i-2} + \delta_{i-1}) + \delta_i) = \dots,$$

where the e-seal includes two parts. One part is the e-seal image, and the other
25 part is the digest of the content with respect to that e-seal, which is coded in the
form of a watermark. The formula can be re-written until the first signer, and then
the digest of the content is known with respect to the i^{th} signer containing
“signatures” of all content of the document at the time of that person’s signing.

- 30 3) Since the digest with respect to each e-seal is different, there is no confusion of on the order of signing of the document. On the other hand, people tend to place an e-

seal at a location that is near that person's addition to the document. This is another cue of the signing order.

2.2.2 "Digest" of the Document

- 5 The embodiments of this invention work for both electronic and printed paper versions of a document. The "digest" of the document content is able to be readily derived from both the electronic and paper versions of the document, and the derived digests are the same or quite similar. The "digest" of a document's content can be defined as a condensed representation of the document having a size sufficiently small
10 so the digest can be embedded into the e-seal image. There are two important desired properties for the digest generation function. Firstly, the digest must be sensitive to content changes, including changes that may be quite small. Secondly, desirably the digest is sensitive to spatial locations so that the location of changes can be detected as well.
- 15 There are many applicable methods to derive digest from documents either in electronic and in paper format. The digest can be formally represented as "Digest = M (Content)", or "Digest = M(Key, Content)", where M stands for a mapping function and "Key" is a secret value shared between the issuer and the verifier. Given below are a few examples of digesting techniques, however, it will be apparent to
20 those in the art in view of this disclosure that other methods may be practised without departing from the scope and spirit of the invention. The examples include:
- 1) In cryptography, a message digest can be generated using a secure hash algorithm. For a digest 128-bits long, approximately 2^{128} messages must be tried before
25 finding two that have the same digest C. Kaufman, R. Perlman and M. Speciner, Network Security, Private Communication in a Public World, PTR Prentice Hall, Englewood Cliffs, New Jersey, 1995, describe details of such secure hashing algorithms. Consequently, it is impractical to find two messages having the same digest. Clearly, a cryptographic digest is suitable to electronic multimedia
30 document, where the document I_s content is digital and has a crisp definition for "same" and "different". A cryptographic digest is also applicable to a document with text content where optical character recognition (OCR) works well to convert

A secure hashing algorithm is a pseudo-random mapping function. A single bit error in the content may result in a large difference between the digests. Therefore, the content of the document must be error-free during transmission, storage, and format conversion.

- 2) A simple digest of a document (e.g. degree certificate) can be derived by selection of a few key document items including the recipient, the name of the school, the name of the degree, and the date. Also, a simple way to verify both electronic and paper certificates is to manually input those items.
- 3) The content of a picture has a different form when compared with text. The representation of the text is exact. A one bit change in the content of text results in differences of the text and, possibly, changes of meaning as well. On the other hand, the interpretation of picture is not precise. For example, the content of a facial image may not change even if the image data is reduced from 8 bits per pixel to 4 bits per pixel. Therefore, a “feature measure” can be used to represent the content of a picture. Feature measures are extracted from a picture to capture the most salient features of the image. A typical example of feature measures for facial images is the eigenface. A. Pentland, “Eigenface for recognition”, Journal of Cognitive Neuroscience, Vol. 3, pp 59-70, 1991 provides detailed information on this topic. Other examples include Fourier descriptors, projections, and vector quantisation (VQ) representation. R. C. Gonzalez and R. E. Woods, Digital Image Processing, Addison-Wesley Publishing Company, Reading, 1993 describe such methods. Since feature measures capture the salient features of a picture, a print-and-scan process does not result in much change to the measure. Therefore, detection of changes can be made between an electronic document and the corresponding printed version using a pre-determined threshold. Feature measures can be used as a digest for the picture both in electronic and paper form, as well as for other non-picture data in raster format.

5

- 10

15

20

25

- 30

- **Step 2:** Each block is classified into one of a number of predetermined classes. The classification can be done in either the spatial or transform domain using either original block data or measures extracted from the block. For example, if vector quantization method is adopted, the block must be matched against a pre-determined codebook. This can be also viewed as classification. For the case of a transform domain method, first, the blocks are transformed into the Cosine transform domain. Texture energy, directionality, fineness and dispersion measures can be derived for each block. Using these four measures, the block is classified into one of, say, 16 classes (16 is merely illustrations and both larger and smaller numbers of classes can be practised). For example if the block data in Cosine transform domain is represented as $F(u, v)$, or, $F(r, \theta)$, the four measures are defined as follows:
- **Step 3:** The digest of the document is determined or formed to be an array of class labels.

$$Energy = \sum_u \sum_v |F(u, v)|, \text{ where, } F(0, 0) = 0$$

$$Direction = \sum_u \sum_v \tan^{-1}(u/v) |F(u, v)| / Energy$$

$$Fineness = \frac{\int_0^{\pi/2} d\theta \int_3^4 F(r, \theta) |dr| \int_0^{\pi/2} d\theta \int_3^4 dr}{\int_0^{\pi/2} d\theta \int_1^2 F(r, \theta) |dr| \int_0^{\pi/2} d\theta \int_1^2 dr}$$

$$Dispersion = - \int_0^{\pi/2} P_r(\theta) \log P_r(\theta) d\theta, \text{ where, } P_r(\theta) = \int_0^R |F(r, \theta) dr| / Energy$$

- **Step 4:** For a document to be verified, a document image is processed the same way, using the same class parameters (or code book) as in step 2 to derive the digest. The derived digest is matched against the embedded digest. Class label changes of blocks indicate that modifications have occurred in those blocks.

Class definition (or codebook determination) is an important aspect of this method and can be defined for each individual document, or for a group of documents. If blocks are classified in the spatial domain, the class definition is similar to defining a code book in vector quantization. As an example, consider a class definition in the Cosine transform domain as follows:

- **Step 1:** Choose an appropriate block size. Collect document images that can represent the group of document the classes definition apply to.
- **Step 2:** For all document images, transform each block into Cosine transform domain and extract measures to represent characteristics of those blocks.
- 5 • **Step 3:** Decide the number of classes n_cls , according to the tolerance of modifications of the application: the more classes, the smaller are the modifications that can tolerated.
- **Step 4:** Use a clustering algorithm (e.g. K-Mean) to cluster all blocks into n_cls clusters.
- 10 • **Step 5:** The class definition for the given document image data set is made up of cluster centers and cluster labels.

2.2.4 Authenticity Protection of the Digest and Key Management

As mentioned above, the digest of a document content is embedded into the e-seal in the form of a watermark. The watermark is used to verify the authenticity of the document content. For this purpose, the authenticity of the digest is protected through cryptographic means before the digest is embedded into the watermark.

Cryptographic concepts and terminology are described Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 20 1996.

Three techniques A), B), and C) are set forth hereinafter:

- A) Authenticity protection of the digest using symmetric key encryption can be used. s is a secret key shared between the issuer and the verifier. Also, $E(s, Digest)$ denotes the encryption of a Digest under the key s , and $D(s, Ciphertext)$ is decryption of Ciphertext under the key s .

The operations performed by the issuer include:

- i) Compute the digest from the document content: $Digest = M(Content)$;
- 30 ii) Encrypt the digest under the secret key: $Ciphertext = E(s, Digest)$; and
- iii) Embed the Ciphertext into the watermark.

The operations performed by the verifier include:

- i) Extract the ciphertext from the watermark and denote the extracted ciphertext as $Ciphertext'$;
- ii) Decrypt the extracted ciphertext under the shared secret key: $Digest' = D(s, Ciphertext')$;
- iii) Compute the digest, $Digest''$, from the document content, $Content''$:
 $Digest'' = M(Content'')$;
- iv) Compare the $Digest'$ with $Digest''$. and if the “distance” between $Digest'$ and $Digest''$ is within a pre-defined threshold, accept the document as authentic; otherwise reject the document.

B) Authenticity protection of the digest of a document content can be provided using Message Authentication Check (MAC). Let s be a secret key shared between the issuer and the verifier. The MAC of the digest of a document is defined as $MAC = H(s, Digest)$, where $H()$ is a one-way hash function.

The operations performed by the issuer include:

- i) Compute the digest of the document content: $Digest = M(Content)$;
- ii) Compute MAC of the digest: $MAC = H(s, Digest)$; and
- iii) Embed MAC into the watermark.

The operations performed by the verifier include:

- i) Extract the MAC from the watermark and denote it as MAC' ;
- ii) Compute digest from the document content: $Digest'' = M(Content'')$;
- iii) Compute $MAC'' = H(s, Digest'')$; and
- iv) Compare MAC' with MAC'' and, if the two are equal, accept document as authentic; otherwise reject the document.

C) Authenticity protection of the digest can be provided using a digital signature, s and p are the private and public key pair of an issuer for a given digital signature scheme. The digital signature of the issuer on the digest of a document can be denoted as $SIG = S(s, Digest)$. There are two types of digital signature schemes --

digital signature schemes with an appendix and digital signature schemes with message recovery. Without loss of generality, the latter type of digital signature schemes is assumed in the description below. Examples of such schemes are RSA, Rabin, and Nyberg-Rueppel. Generalization to the former type of digital signature schemes is straightforward for those skilled in the art. Further, the verifier is assumed to obtain the public key of the issuer in an authentic manner.

The operations performed by the issuer include:

- i) Compute the digest from the document content: $\text{Digest} = M(\text{Content})$;
- ii) Compute digital signature of the digest: $\text{SIG} = S(s, \text{Digest})$;
- iii) Embed SIG into the watermark.

The operations performed by the verifier include:

- i) Extract the digital signature from the watermark and denote it as SIG' ;
- ii) Recover the digest from SIG' using issuer's public key: $\text{Digest}' = R(p, \text{SIG}')$, where $R()$ is the message recovery function of the digital signature scheme;
- iii) Compute digest from the document content: $\text{Digest}'' = M(\text{Content}'')$;
- iv) Compare Digest' with Digest'' and if the "distance" between Digest' and Digest'' is within a pre-defined threshold, accept document as authentic; otherwise, reject the document.

Note that approaches A) and B) are suitable for situations where the issuer and the verifier trust each other, while approach C) can be used in situations where the issuer and the verifier do not trust each other.

Keys used in watermark embedding (e.g. address and parameters) and in digest derivation (eigenfaces ...) are generated by the authorities and stored in the file of the document.

2.2.5 Watermark Embedding

Unlike circumstances involving copyright protection, people do not ordinarily try to remove watermarks from an e-seal, since such people need to provide evidence establishing the originality of the document. Thus, non-perceptibility and robustness are not a major issue. Therefore, a spatial domain embedding method may be more preferable than a spectrum domain technique. The spatial domain method is simple and has a large capacity.

There are many possible watermarking techniques applicable to document content digest embedding in accordance with the embodiments of the invention. M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia Data Embedding and Watermarking Technologies", Proc. of the IEEE, Vol.86, No.6, June/1998. pp. 1064-1087 provide a review of watermark technologies.

The required properties for watermark embedding methods for document authentication are:

- 1) A large capacity to store document digests, the size of which varies from application to application, and.
- 2) Robust to print-rescan processes, which is a necessary step for verification of the paper version.

The embodiments of the invention can utilise, but are not limited to, a simple technique shown in Fig. 3. The digest 300B is embedded in a region of the e-seal image 300A. Part of the boundary of the watermark region 300B is the boundary of the original image content 300. The boundary 300B is recorded in the document file so as to facilitate watermark extraction in the verification process. This boundary is "content-dependent" and closely couples the watermark 300B and the seal image 300A. Principally, the watermark region 300B can be of any shape and at any location, depending on the needs of the application, as long as the watermark region does not affect the perception of the major image content 300A.

In this method, the digest 300B is coded as binary modulation of S component in HSV color space in Fig. 3. Other possible modulations to other components or in

other color space are also valid. To reduce the error rate, either an error correction code can be used or the digest can be encoded with more pixels. When extracting the watermark 300B from a re-scanned document, there is no problem in recovering the information if the resolution of the scanner is high enough.

5

2.3 Optical Sensible Component

The visible e-seal provides an immediate warning to people regarding document legitimacy protection. Together with a visible seal, the optical sensible component provides secure protection for a printed document and easy verification by means of standard optical devices, such as a special lens or a commonly available device including a photocopier.

10

Any of a large number of optically sensible components can be applied in the embodiments of the invention. Preferably, either of two methods for embedding optical sensible component into a document can be used:

15

- 1) Directly embed certain secure elements into the content of the document. By detecting some "holes" in the frequency-domain, the secure elements can be embedded into these holes and later detected by an optical lens specially designed to match this particular class of document.
- 2) The visual elements of the document can be modulated to make the document sensitive to a particular lighting scan along a pre-defined direction by either increasing the resolution or changing the color of the document. In this case, the detector can be a commercially available photocopier or scanner.

20

25

2.4 Document Structures

Fig. 4 depicts the layout of a one page document400, including a content region 420 and two e-seal parts: a logo 410 and signature 430 (and preferably a serial number). The content region 420 can be further subdivided into several regions, each of which may contain different media, such as text, graphics, a table and/or a picture.

30

2.4.1 Landmarks or Frames for Easy Location

Frames 410, 420, 430 can be added as landmarks for the easy location of content 420 and e-seal regions 410, 430. Other forms of a landmark can be used instead of frames without departing from the scope and spirit of the invention.

5 2.4.2 Multiple Parts of E-seal

There may be multiple parts of an e-seal. A typical example is a formal document 430, which includes two parts: a formal document header 410, and a signature and/or a seal 430 of an organization. The document header 410 may contain the name and logo of the organization. Classification and serial number of the document are usually
10 printed in a place near the header as well. However, this can be part of the content 420 preferably. The visible information is embedded as watermark into the logo image 410 for protection. Commonly, a paper document to be a valid document must contain both a header and one or more signatures. Clearly, it is desirable that all images in the e-seal are watermarked to protect the ownership, although this need not
15 be the case.

2.4.3 Multiple Pages

For a multiple page document, an e-seal can be inserted to every page. Preferably a page number (numbered as current number – total number) is included in the
20 document and considered as to be part of document content.

2.4.4 File of Authorized Document

For each authorized document, a file containing necessary information is created and stored for further reference. The information contained in the file includes a key for
25 authenticity protection of the digest and/or embedding, the size of the e-seal, parameters for an optically sensible component, the names of the signing persons, and the like. The file is stored with an authority or a trusted third party. A verification process can access the file.

30 3. Protection and Verification Process

3.1 Electronic Document Signing Process

Fig. 5 illustrates the protection process for an electronic document according to a first embodiment of the invention. When a person starts the document signing process, the person needs to unlock the person's e-seal 534 using either a password or biometrics (fingerprint, face, etc). For a given electronic document with single signing person,

5 verification module 510 for the verification of a previous e-seal is not applied to the electronic document or e-document 510 and the digest of the document content is generated by digest generation module 520, either with a key or without a key. A key is obtained to encrypt the digest if necessary. Address and parameters are chosen as a key 532 provided to the watermark embedding module 530 to embed the digest (as

10 well as the time when the watermark is embedded) as a watermark into the e-seal image 534 and provide authentication of E-document file 542. Landmarks for easy location of e-seal and content can be added. The final module 540 of the process includes or adds information including the e-seal to the electronic document 512 and adds landmarks for verification and printing to provide an authenticated E-document

15 542 and an E-document file 544.

In case of multiple signing persons, at the time of the n^{th} signing person, verification is conducted using module 510 to validate all previous e-seals. The person's additional information is added to the document, a digest derived with respect to that

20 person, and the digest encrypted and embedded. Information relating to the signing (adding the e-seal of that person) is added to the file of the electronic document.

For many applications, the content of the document includes main content, classification number, serial number, page number and all other information contained

25 in the document.

For applications requiring high security, personal authentication of the signing person is necessary. This can be done using a password, a biometrics such as fingerprint and face, or smartcard. After successful personal authentication, the system does the

30 following: unlocks the e-seal image, signs the document, and charges the cost to the person's account.

3.2 Verification Process for Electronic Document

Fig. 6 illustrates the verification process for an authenticated electronic document 542 containing an e-seal and the corresponding electronic file 544 as input. First, the e-seals are located and verified by module 610. With information from the file, the watermark of each e-seal is extracted and decrypted to get the original digest. The digest of the content with respect to each e-seal is extracted from the electronic document, and compared with the digest extracted from the e-seal by module 620. The verification is successful if there is no difference or the difference is under a pre-defined threshold. In certain cases, validation of the e-seal image may be required to check the true ownership (of the e-seal) by extracting the copyright protection watermark in module 630 to produce verification result 644. If the verification result 644 is "Yes" or "true", this indicates that the authenticated electronic document is an original. If the verification result 644 is "No" or "false", this indicates that the document is not an original or is a forgery and the forgery is likely located at location (x,y).

3.3 Printing of Electronic Document

Printing of an electronic document 542 to get an authenticated printed copy 734 is controlled by the printing method shown in Fig. 7. The legitimacy of the electronic document is verified by verification module 710. If the verification is successful, an optical sensible component is added (preferably with a copy number) by adding module 720. The document is then printed by module 730. A serial number of the printed copy can be added to the document file, as well to the printed copy. The optical sensitive component is added to the e-seal of the last signer, which provides overall protection of the document including previously signed e-seals.

A valid printed document can be only generated by the printing method of Fig. 7. This ensures that people cannot edit and then print the electronic document using any printing functions. By controlling the usage of the printing function, the legitimacy of the printed document can be secured to a large extent using the optically sensible component.

There are several ways to control the printing function. In this embodiment of Fig. 7, since there must be verification before printing, the printing function is controlled by parties who have verification rights and the verification is well facilitated. Following are two ways of controlling the printing function.

5

- 1) On-line control: A user logs on through a secure network and requests printing of a particular electronic document. After successful user verification by the authority or the trusted third party, the authority or trusted third party verifies the document and sends the printing function together with necessary data over to the user's site. The printing function prints the document on the user's printer. The document being printed, the portion of the data that has been printed already can be destroyed as the printing process is in progress. This can be done by erasing the memory containing that data portion progressively.

10

15

- 2) Verification and printing agent: An authorized agent may have a special printing device. The printing device can be either on-line connected to the authority or off-line. In the off line case, data and functions are preloaded into the device. The device prints out the document when a user is authorized. When the device runs in an on-line mode, the process is similar to the first approach. Partial data and function can be stored with the device depending upon the degree of security the device has.

20

3.4 Verification Process for Printed Document

25 There are three levels of verification for a printed document. As shown in Fig. 8, the verification starts with a printed document 734 to be verified, together with certain information about the document contained in a file of the document 544. The difference in verification of the electronic and paper document 644, 734 is that the paper document 734 can be verified by visual inspection, and the paper document 734 has to be scanned to convert it to digital form before the paper document can be verified the same way as electronic document 544. The first level of verification is the visual inspection of the e-seals by module 810, the second level verification is the verification of the optically sensible component by module 820. The verification

30

5

10

20

25

There are many possible products and services that can be created from the embodiments of the invention. Listed below are two examples. The basic concepts are applicable to numerous other similar applications.

30

Currently, official letters and many other secure documents are delivered physically, via postal services or express deliveries such as Federal Express. The embodiments of the invention facilitate the electronic delivery of a trusted copy of a document. That is, a recipient can receive a trusted document either in electronic and/or in paper form.

5 There are two types of settings described below.

The first setting involves the sender's organization being an authorized identity and having set up a computer system, with the functionality described above:

- 10 1) The sender prepares an electronic document by either editing an electronic document or scanning in a paper document. The sender then logs into to the organization's computer system, gets authorized, unlocks the person's e-seal, signs the document, and sends the document to the recipient while specifying if the server wants the recipient to receive the document in electronic and/or paper format.
- 15 2) When the recipient receives a notification (organization-organization or organization-individual) or when the recipient requests a document (tickets, coupon, gazettes, receipts...), the recipient logs into the sender's system, gets the electronic document, and/or prints out the paper document. When the document is printed, the printing function from the sender's system is invoked, and the sender's e-seals and optical sensitive
- 20 component are added to print a trusted copy.

The second settings involves a document being sent through a service center:

- 25 1) The sender prepares an electronic document by either editing an electronic document or scanning in a paper document. The sender logs into a service center, gets identified, unlocks the person's e-seal, signs the document, and sends the document to the recipient while specifying if the sender wants the recipient to receive the document in electronic and/or paper format.
- 30 2) When the recipient receives a notification (organization-organization or organization-individual) or when the recipient requests a document (tickets, coupon, gazettes,...), the recipient logs into the service center,

gets the electronic document, and/or prints out the paper document. When the document is printed, the printing function from the service center is invoked, and the sender's e-seals and optical sensitive component are added to print a trusted copy. Alternatively, the service center can add a notarization seal and optical sensitive component to certify the true copy.

4.2 Certification and Notarization

Currently, certification and notarization for official documents and papers such as graduate certificates, marriage certificates, and transcripts are all done in paper form. For example, a university student in Asia applying for graduate admission to a US university has to get all of that person's certificates and transcripts initiated by the university authority and sent through the public mailing system. A significant problem is that there are many universities in the world. Further, it is difficult for an admission official to judge the legitimacy of those documents. Still further, the student does not know if the documents the student sent are acceptable.

The product of certification and notarization here applies to all types of documents, including, but not limited to, birth certificates, marriage certificates, degree certificates, and official letters. Degree certificates are used as an example in the following description. The embodiment of the invention is directed to the framework and technologies for operation of a certification/notarization service center.

The service center 910 shown in Fig. 9 provides on-line services to document issuers 930 (e.g. the university the student obtained the degree from), document owners 920 (graduates), and document recipient 940 (the university the student is applying for a higher degree admission). Processes for various requests are as follows:

Firstly, an owner 920 requests an electronic degree certificate through the service center 910 with the indicated issuer 930 and the following steps are performed:

- 1) An owner 920 logons to the webpage of the service center 910, gets registered if not yet already done, and fills in a request form.

- 2) The service center 910 communicates with the issuer 930 about the request and arranges business links between the service center 910 and the issuer 930 if not yet already done.
- 3) The issuer 930 connects to the service center 910, issues an electronic degree certificate for that owner 920, and sends the certificate to the owner 910 through the service center 910.
- 4) The service center 910 keeps a record of the certificate, which is collected during the issuing process and is enough for the verification service.
- 5) The owner 920 can choose to either keep the e-certificate, or rent a secure deposit box to keep the certificates in the service center 910.

Secondly, an alternative way is that the owner 920 brings in a paper document (degree certificate) to the service center 910 and requests an electronic certificate service, which includes the following steps:

- 1) The service center 910 verifies the legitimacy of the paper document with the original issuer 930 on its capacity, converts the paper document to electronic form, signs on the electronic version and assigns a trust level to the document. For example, the trust level can be high if verified with the original issuer.
- 2) The service center 910 keeps a record of the certificate.
- 3) The owner 920 can choose to either keep the e-certificate, or rent a deposit box to keep certificates in the service center 910.

Thirdly, an owner (student) 920 requests to send an electronic document (degree certificate) to a recipient 940 (the university the student is applying for a higher degree study) and includes the following steps.

- 1) The owner 920 logs into the webpage of the service center 910 and fills in a request form.
- 2) The service center 910 verifies the electronic document and sends the document to the recipient 940 together with service center's e-seal and security statement (level of trust).

- 3) The service center 910 notifies the owner 920 of the status when the recipient 940 has collected the electronic document.

Fourthly, a party can request the service of document legitimacy verification including the following steps:

- 1) The party should register with the service.
- 2) The registered party logs on to the webpage of the service center 910, and sends in the electronic document.
- 3) The service center 910 checks for the record of the document and carries out the verification. If there is no record, the service center 910 contacts the issuer 930 for verification, and then puts the service center's e-seal into the document together with a security statement.
- 4) The service center 910 keeps a record of that document and sends back the electronic document to the registered party.

Fifthly, the service center 910 receives a request to print a hard copy of an electronic document either from an owner 910 or another party.

- 1) The user should registers with the service center 910.
- 2) The user logs into the webpage of the service center 910 and sends in the electronic document.
- 3) The service center 910 performs verification on the electronic document, assigns a trust level to the document, and prints a copy together with the center's e-seal and a dedicated optical sensitive component.

Sixthly, the service center 910 receives a request for legitimacy verification of a printed copy involving the following steps:

- 1) The service center 910 verifies the validity of the e-seals by visual inspection.
- 2) The service center 910 verifies the validity of the optically sensitive component.

- 3) The service center 910 scans in the paper document, and verifies the document legitimacy by checking the document content digest and ownership of the e-seal (if necessary).

5 In the sixth process, the service center 910 need only keep a record of the document that is necessary for verification services. The record is created and the data is collected when the document is signed using the services provided by the service center 910. That is, the service center 910 does not keep a copy of the whole document. By doing so, the authority of the issuer 920 is well respected, and the
10 privacy of the owner is protected. When a user chooses to rent a deposit box in the service center 910, the deposit box is protected by the user. The service center 910 does not have any right to access the content of the deposit box.

The owner 920 of the certificates can choose to send the e-certificates to anyone
15 directly.

The service center 910 is advantageous for a number of reasons:

- 1) There are many document issuers in the world, and there is little or no information available about issuers and those issued documents.
20 Consequently, there is hardly any effective means for legitimacy verification.
- 2) It is time consuming and costly for owners to send paper documents and also to provide official evidence regarding the legitimacy of the documents.
- 25 3) It is not efficient for each issuer to provide a verification service regarding the legitimacy of certificates and other documents.

4.3 Electronic Check

Checks or negotiable instruments are used and preferred by many people to pay their
30 bills. The parties involved are a payer, a payee, a payer's bank, a payee's bank and the service center. An electronic check services product is as follows:

Firstly, the payer issues a check involving the following steps:

- A) The payer registers with the service center 910 for the service.
- B) The payer logs on to the service center 910 through the center's webpage.
- 5 C) The payer fills in the form for payment and signs the form using the same means as with the bank (pin, fingerprint, face, or others). The form includes information about the payer's bank and bank account, the person's name and identification number, the payee's name, amount, and the date of the payment.
- 10 D) The service center 910 links to the payer's bank for validation.
- E) The service center 910 signs the check with both the payer's and service center's e-seals and sends the check to the payee.
- F) After the payee picks up the check, the service center 910 notifies the payer.
- 15 G) The payer can choose to print out the check using the printing function provided by the service center 910, and personally give the check to the payee. The printed check has security feature of the payer's bank, the signature of the payer, the seal and optical sensitive component from the service center 910 and is trusted.

20 Secondly, the payee claims the check involving the following steps:

- A) The payee registers with the service center 910.
- B) The payee logs on to the service center's webpage.
- C) The payee sends in the electronic check to the service center 910.
- D) Alternatively, the payee can send the check to payee's bank, and the
25 bank scans in to read any required information from the check, and sends the information to the service center 910.
- E) The service center 910 verifies the check with the original form filled in by the payer.
- F) The service center 910 sends the check to the payee's bank with
30 verification result.
- G) The payer's bank accepts the check and commits the transfer on the due date indicated in the check.

- 5

4.4 Service Center for Secure Document with Multiple Signers

- 30

- F) Upon a request, the service center 910 verifies and prints out a paper copy of the document with an optical sensitive component that is generated by the service center 910 for that document. The optical sensitive component is coupled with the last signer's e-seal.

5

For the case of multiple signers for an official document, the system server of an organization can be used rather than a service center and involves the following steps:.

- 10 A) An official document (e.g. a design document of a building) is created by a proposer.
- B) The proposer logs into the system server. With that person's private key, the proposer signs and sends the document to the next person for verification/approval through the system server.
- 15 C) The system server notifies the next person of the arrival of the document, and the person signs the document.
- D) The system server creates a record of the document and files the record for further verification.
- E) The final signed document is filed in an archive of the organization.
- 20 F) Upon request, the system server verifies and prints out a paper copy of the document. The printed copy has optical sensitive component added to the document. The optical sensitive component is from the system server, designed for this particular document, and coupled together with an e-seal of the last signer.

- 25 The embodiments of the invention are preferably implemented using general-purpose computers. In particular, the processing or functionality of Figs. 1-9 can be implemented as software, or a computer program, executing on a computer. The method or process steps of protecting the legitimacy of electronic and corresponding printed documents are effected by instructions in the software that are carried out by
- 30 the computer. The software may be implemented as one or more modules for implementing the process steps. A module is a part of a computer program that usually performs a particular function or related functions. Also, as described

hereinbefore, a module can also be a packaged functional hardware unit for use with other components or modules.

In particular, the software may be stored in a computer usable or readable medium, including a floppy disc, a hard disc drive, a magneto-optical disc drive, CD-ROM, magnetic tape or any other of a number of non-volatile storage devices well known to those skilled in the art. The software is preferably loaded into the computer from the computer usable medium and then carried out by the computer. A computer program product includes a computer usable medium having such software or a computer program recorded on the medium that can be carried out by a computer. The use of the computer program product in the computer preferably effects an advantageous system for virtual commodity trading.

The computer system can be connected to one or more other computers via a communication interface using an appropriate communication channel such as a modem communications path, a computer network, or the like. The computer network may include a local area network (LAN), a wide area network (WAN), an Intranet, and/or the Internet.

Numerous configurations of computer systems can be employed without departing from the scope and spirit of the invention. Computers with which the embodiment can be practiced include IBM-PC/ATs or compatibles, the Macintosh (TM) family of PCs, Sun Sparcstation (TM), a workstation or the like. The foregoing is merely exemplary of the types of computers with which the embodiments of the invention may be practiced.

Typically, the processes of the embodiments are resident as software or a program recorded on a hard disk drive as the computer readable medium, and read and controlled using the computer system. In some instances, the program may be supplied to the user encoded on a CD-ROM or a floppy disk, or alternatively could be read by the user from the network via a modem device connected to the computer, for example. Still further, the software can also be loaded into the computer system from

5

10

15

1. An electronic document for reproduction of a corresponding printed document capable of having the legitimacy of said electronic document protected, said printed document being a printed version of said electronic document, said electronic document including:

a content digest for said content said original document in electronic form;

an optically sensitive or sensible component added to said authenticated document for printing using a trusted printing process, said optically sensitive or sensible component containing information for indicating copying or modification of
15 said printed document in a copy or modified version of said printed document.

20

3. The electronic document according to claim 2, wherein said content digest is encrypted prior to watermarking said visible seal.

5. The electronic document according to claim 1, wherein said content digest is a condensed representation of said original document generated by a step
30 selected from the group consisting of:

hashing said content using a secure hashing process;
selecting key items of said content; and

6. The electronic document according to claim 1, wherein said content digest is a condensed representation of said original document generated by block-wise digest derivation applied to said content, each block having a predetermined size and shape, said content digest including an array of labels with each label being dependent upon a classification of a corresponding block of said content.

8. The electronic document according to claim 1, wherein said optically sensitive or sensible component includes a serial number for said electronic document.

10. The electronic document according to claim 1, further including a
25 second e-seal having:
content for said second e-seal including said content of said original document
and said (first) e-seal; and
a visible seal of an authority and a content digest dependent upon said content
of said second e-seal embedded in said visible seal.

5 12. A printed document reproduced from an electronic document capable
of having the legitimacy of said printed document protected, said printed document
being a printed version of said electronic document, said printed document including:
rendered content of an original document;

an optically sensitive or sensible component rendered in said authenticated document using a trusted printing process, said optically sensitive or sensible component containing information for indicating copying or modification of said printed document in a copy or modified version of said printed document.

14. The printed document according to claim 13, wherein said content digest is encrypted prior to watermarking said visible seal.

16. The printed document according to claim 12, wherein said content
30 digest is a condensed representation of said original document generated by a step
selected from the group consisting of:

hashing said content using a secure hashing process;

17. The printed document according to claim 12, wherein said content
5 digest is a condensed representation of said original document generated by block-
wise digest derivation applied to said content, each block having a predetermined size
and shape, said content digest including an array of labels with each label being
dependent upon a classification of a corresponding block of said content.

19. The printed document according to claim 12, wherein said optically
15 sensitive or sensible component includes a serial number for said printed document.

at least one of two or more pages and multimedia information in said content;

one or more landmarks for locating at least one of said content, said e-seal, and other document components.

content for said second e-seal including said content of said original document and said (first) e-seal; and

30

23. A method of protecting the legitimacy of an electronic document and a corresponding printed document, said printed document being a printed version of said electronic document, said method including the steps of:

adding an optically sensitive or sensible component to said authenticated document for printing using a trusted printing process, said optically sensitive or sensible component containing information for indicating copying or modification of said printed document in a copy or modified version of said printed document.

20

25 26. The method according to claim 25, wherein at least one of an
embedding address, shape, and boundary of said watermark is a key for encrypting
said content digest, watermarking said e-seal, or both..

30

hashing said content using a secure hashing process;

28. The method according to claim 23, wherein said content digest is a condensed representation of said original document generated by block-wise digest derivation applied to said content, each block having a predetermined size and shape, said content digest including an array of labels with each label being dependent upon a classification of a corresponding block of said content.

30. The method according to claim 23, wherein said optically sensitive or
15 sensible component includes a serial number for said electronic document.

32. The method according to claim 23, further including a second e-seal
25 having:
content for said second e-seal including said content of said original document
and said (first) e-seal; and
a visible seal of an authority and a content digest dependent upon said content
of said second e-seal embedded in said visible seal.

33. The method according to claim 23, further including the step of embedding an imperceptible watermark in said e-seal for protecting ownership of the authority of said e-seal.

5 34. An apparatus for protecting the legitimacy of an electronic document and a corresponding printed document, said printed document being a printed version of said electronic document, said apparatus including:

means for generating a content digest for an original document in electronic form;

10 means for authenticating said original document in electronic form using an electronic seal or e-seal, said e-seal including a visible seal of an authority and said content digest embedded in said visible seal;

means for adding an optically sensitive or sensible component to said authenticated document for printing using a trusted printing process, said optically
15 sensitive or sensible component containing information for indicating copying or modification of said printed document in a copy or modified version of said printed document.

20 35. The apparatus according to claim 34, wherein said authenticating means includes means for watermarking said visible seal with said content digest to embed said content digest in said visible seal.

25 36. The apparatus according to claim 35, wherein said authenticating means includes means for encrypting said content digest prior to watermarking said visible seal.

30 37. The apparatus according to claim 36, wherein at least one of an embedding address, shape, and boundary of said watermark is a key for encrypting said content digest, watermarking said e-seal, or both.

means for hashing said content using a secure hashing process;

5 means for selecting key items of said content; and

means for extracting features of said content.

40. The apparatus according to claim 34, wherein said visible seal includes
15 at least one of a document header, a logo or artwork, a graphical symbol, and a
signature.

42. The apparatus according to claim 34, wherein said electronic document includes:

43. The apparatus according to claim 34, further including a second e-seal
having:
30 content for said second e-seal including said content of said original document
and said (first) e-seal; and

a visible seal of an authority and a content digest dependent upon said content of said second e-seal embedded in said visible seal.

44. The apparatus according to claim 34, further including means for
5 embedding an imperceptible watermark in said e-seal for protecting ownership of the
authority of said e-seal.

45. A computer program product having a computer usable medium having a computer readable program code means embodied therein for protecting the legitimacy of an electronic document and a corresponding printed document, said printed document being a printed version of said electronic document, said computer program product including:

computer readable program code means for generating a content digest for an original document in electronic form;

15 computer readable program code means for authenticating said original document in electronic form using an electronic seal or e-seal, said e-seal including a visible seal of an authority and said content digest embedded in said visible seal;

computer readable program code means for adding an optically sensitive or
sensible component to said authenticated document for printing using a trusted
20 printing process, said optically sensitive or sensible component containing
information for indicating copying or modification of said printed document in a copy
or modified version of said printed document.

46. The computer program product according to claim 45, wherein said
25 computer readable program code means for authenticating includes computer readable
program code means for watermarking said visible seal with said content digest to
embed said content digest in said visible seal.

47. The computer program product according to claim 46, wherein said
30 computer readable program code means for authenticating includes computer readable
program code means for encrypting said content digest prior to watermarking said
visible seal.

48. The computer program product according to claim 47, wherein at least one of an embedding address, shape, and boundary of said watermark is a key for encrypting said content digest, watermarking said e-seal, or both..

5

49. The computer program product according to claim 45, wherein said content digest is a condensed representation of said original document generated by computer readable program code means selected from the group consisting of:

- computer readable program code means for hashing said content using a secure hashing process;
- computer readable program code means for selecting key items of said content; and
- computer readable program code means for extracting features of said content.

15

50. The computer program product according to claim 45, wherein said content digest is a condensed representation of said original document generated by computer readable program code means for block-wise digest derivation of said content, each block having a predetermined size and shape, said content digest including an array of labels with each label being dependent upon a classification of a corresponding block of said content.

20

51. The computer program product according to claim 45, wherein said visible seal includes at least one of a document header, a logo or artwork, a graphical symbol, and a signature.

25

52. The computer program product according to claim 45, wherein said optically sensitive or sensible component includes a serial number for said electronic document.

30

53. The computer program product according to claim 45, wherein said electronic document includes:

at least one of two or more pages and multimedia information in said content;
and

one or more landmarks for locating at least one of said content, said e-seal,
and other document components.

5

54. The computer program product according to claim 45, further
including a second e-seal having:

content for said second e-seal including said content of said original document
and said (first) e-seal; and

10 a visible seal of an authority and a content digest dependent upon said content
of said second e-seal embedded in said visible seal.

55. The computer program product according to claim 45, further
including computer readable program code means for embedding an imperceptible
15 watermark in said e-seal for protecting ownership of the authority of said e-seal.

56. A system utilising a network for protecting the legitimacy of an
electronic document and a corresponding printed document, said printed document
being a printed version of said electronic document, said system including:
20 means for generating a content digest for an original document in electronic
form;

means for authenticating said original document in electronic form using an
electronic seal or e-seal, said e-seal including a visible seal of an authority and said
content digest embedded in said visible seal;

25 means for adding an optically sensitive or sensible component to said
authenticated document for printing using a trusted printing process, said optically
sensitive or sensible component containing information for indicating copying or
modification of said printed document in a copy or modified version of said printed
document.

30

005050 0458460

5 58. The system according to claim 57, wherein said authenticating means includes means for encrypting said content digest prior to watermarking said visible seal.

60. The system according to claim 56, wherein said content digest is a condensed representation of said original document generated by means selected from the group consisting of:

61. The system according to claim 56, wherein said content digest is a condensed representation of said original document generated by means for block-wise digest derivation of said content, each block having a predetermined size and shape, said content digest including an array of labels with each label being dependent upon a classification of a corresponding block of said content.

30 63. The system according to claim 56, wherein said optically sensitive or
sensible component includes a serial number for said electronic document.

5 one or more landmarks for locating at least one of said content, said e-seal,
and other document components.

a visible seal of an authority and a content digest dependent upon said content of said second e-seal embedded in said visible seal.

67. The system according to claim 66, wherein said trusted printing or
20 reproduction device is accessible via said network and is remotely located from one or
more of the other components of said system.

68. The system according to claim 56, further including means for
embedding an imperceptible watermark in said e-seal for protecting ownership of the
25 authority of said e-seal.

means for generating an authenticated electronic document, said authenticated
30 electronic document including content of an original document in electronic form, an
electronic seal or e-seal for authenticating said original document in electronic form,

means for generating an optically sensitive or sensible component added to said authenticated electronic document for printing using a trusted printing process, said optically sensitive or sensible component containing information for indicating copying or modification of said printed document in a copy or modified version of said printed document;

means for printing said authenticated electronic document and said optically
10 sensitive component using said trusted printing process dependent upon said verifying
means to provide an authenticated printed document.

71. The system according to claim 70, wherein said legitimacy verifying means further includes means for locating and verifying one or more e-seals in said authenticated electronic document.

25

means for verifying the legitimacy protection of said authenticated printed document based on said electronic document.

30 74. The system according to claim 73, wherein said means for verifying
the legitimacy protection said authenticated printed document further including:

means for extracting a content digest from each of said watermarks and verifying said extracted content digest.

75. A method for protecting the legitimacy of an electronic document and
a corresponding printed document, said method including the steps of:

generating an authenticated electronic document, said authenticated electronic document including content of an original document in electronic form, an electronic seal or e-seal for authenticating said original document in electronic form, said e-seal including a visible seal of an authority and a content digest embedded in said e-seal;

generating an optically sensitive or sensible component added to said authenticated electronic document for printing using a trusted printing process, said optically sensitive or sensible component containing information for indicating copying or modification of said printed document in a copy or modified version of said printed document;

verifying the legitimacy of said authenticated electronic document;
printing said authenticated electronic document and said optically sensitive component using said trusted printing process dependent upon said verifying step to provide an authenticated printed document.

25

76. The method according to claim 75, wherein said legitimacy verifying step includes the step of verifying a watermarked digest of content against a corresponding one of one or more e-seals included in said authenticated electronic document.

30

5 78. The method according to claim 76, wherein said legitimacy verifying step further includes the step of verifying the validity of each of one or more e-seals included in said authenticated electronic document.

80. The method according to claim 79, wherein said step for verifying the legitimacy protection said authenticated printed document further includes the steps of:

81. A computer program product having a computer usable medium
25 having a computer readable program code means embodied therein for protecting the
legitimacy of an electronic document and a corresponding printed document, said
computer program product including:

computer readable program code means for generating an authenticated electronic document, said authenticated electronic document including content of an original document in electronic form, an electronic seal or e-seal for authenticating said original document in electronic form, said e-seal including a visible seal of an authority and a content digest embedded in said e-seal;

5

au

10

15

20

25

30

of

5 computer readable program code means for visually inspecting said visual seal
of each of said one or more e-seals;

computer readable program code means for scanning said authenticated
10 printed document and extracting a watermark from each of said one or more e-seals;
and

15 87. A method of trusted document delivery via a network, said method
including the steps of:

verifying the identity of each party;

20 providing means for a party to sign an original document;

sending a protected, signed electronic document from a sending party at a first location to a receiving party at a second remote location of said network;

30 receiving said sent protected electronic document at said second remote
location of said network; and

88. The method according to claim 87, further including the steps of:
5 verifying the legitimacy of said sent protected electronic document at said second remote location of said network to ensure the legitimacy of a document to be printed;

printing a copy of said protected electronic document using a trusted printing process.

establishing a secure network with an issuer, an owner and the recipient of the document;

delivering a trusted copy of the document to the recipient.

25

establishing a secure network link from a service center to a payee, a payer, and one or more respective banks;

claiming said check for the payee;

refusing the payment if the check is not legitimate.

5 documents with multiple signing parties including the step of:

signing said electronic document in either a serial or parallel manner.

using a scanning process.

15 legitimacy of said sent protected electronic at a location of said network.

means for a party to sign said original document.

5

An electronic document (200) and a corresponding printed document capable of having their legitimacy protected, and a method, an apparatus, a computer program product and a system for protecting the legitimacy of electronic and printed

15

20

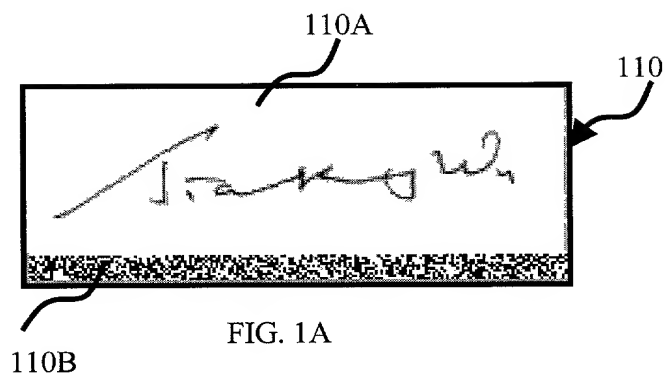


FIG. 1A

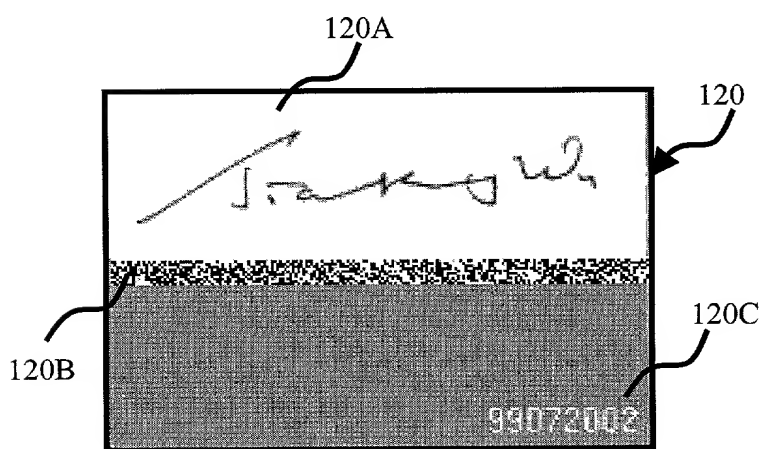


FIG. 1B

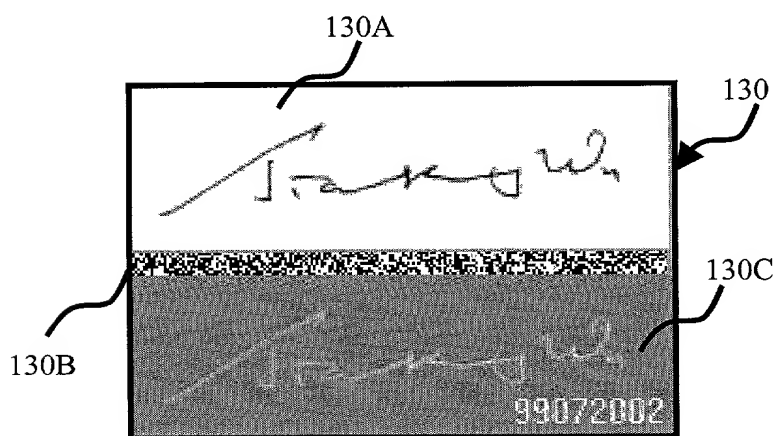


FIG. 1C

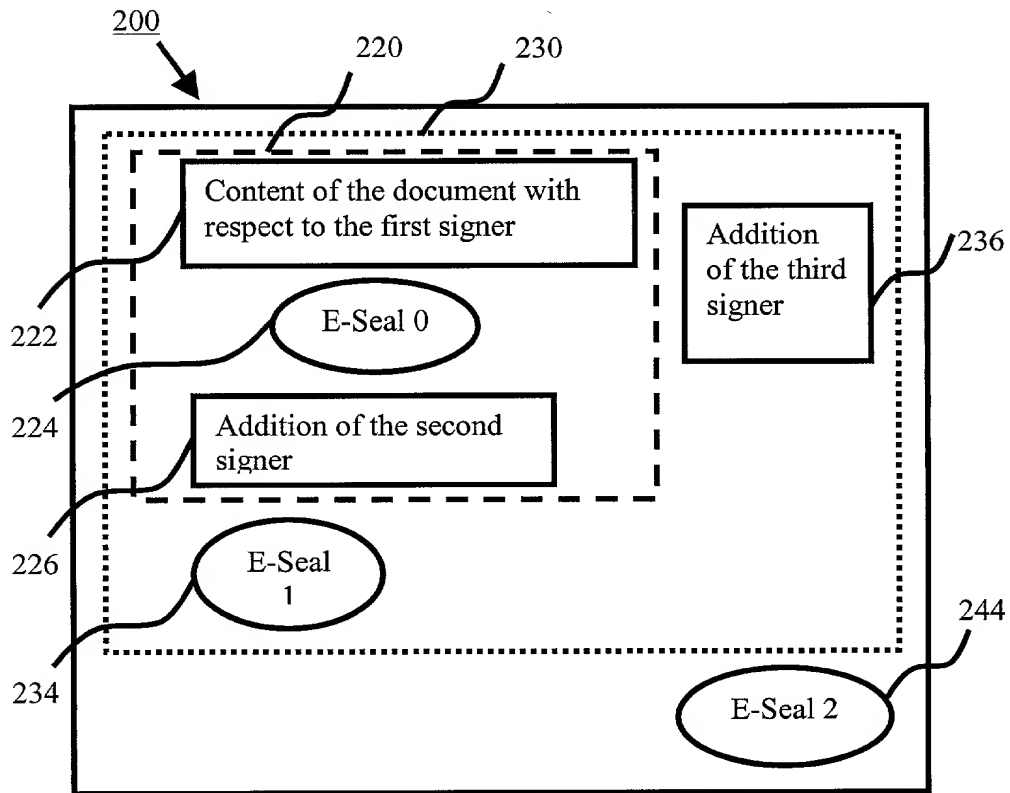


FIG. 2



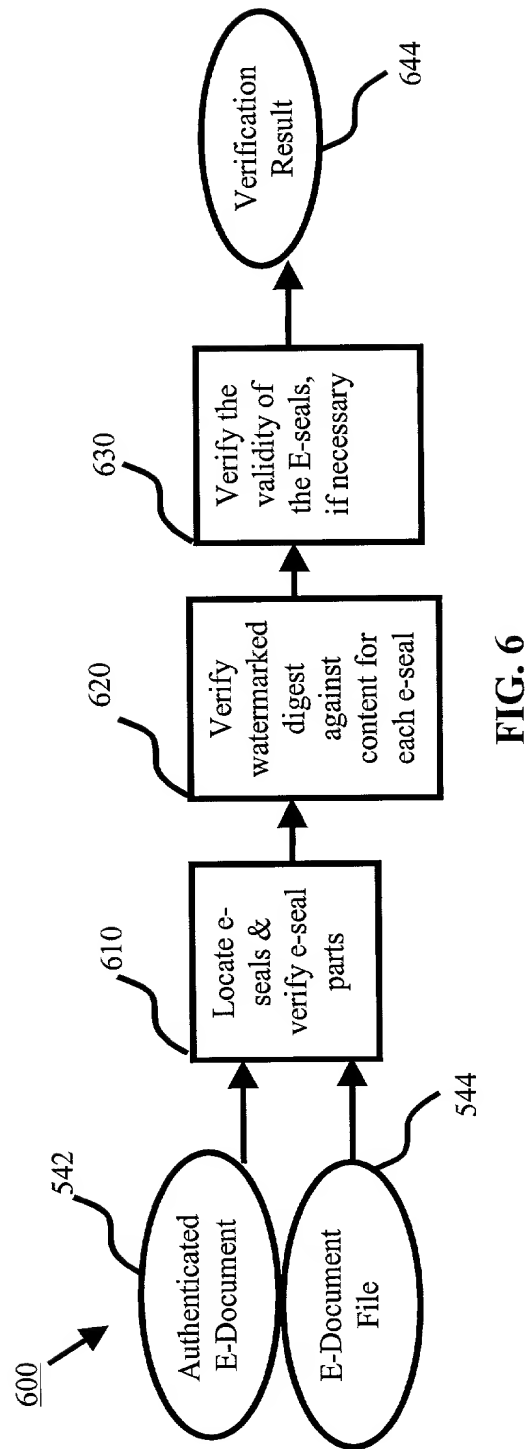
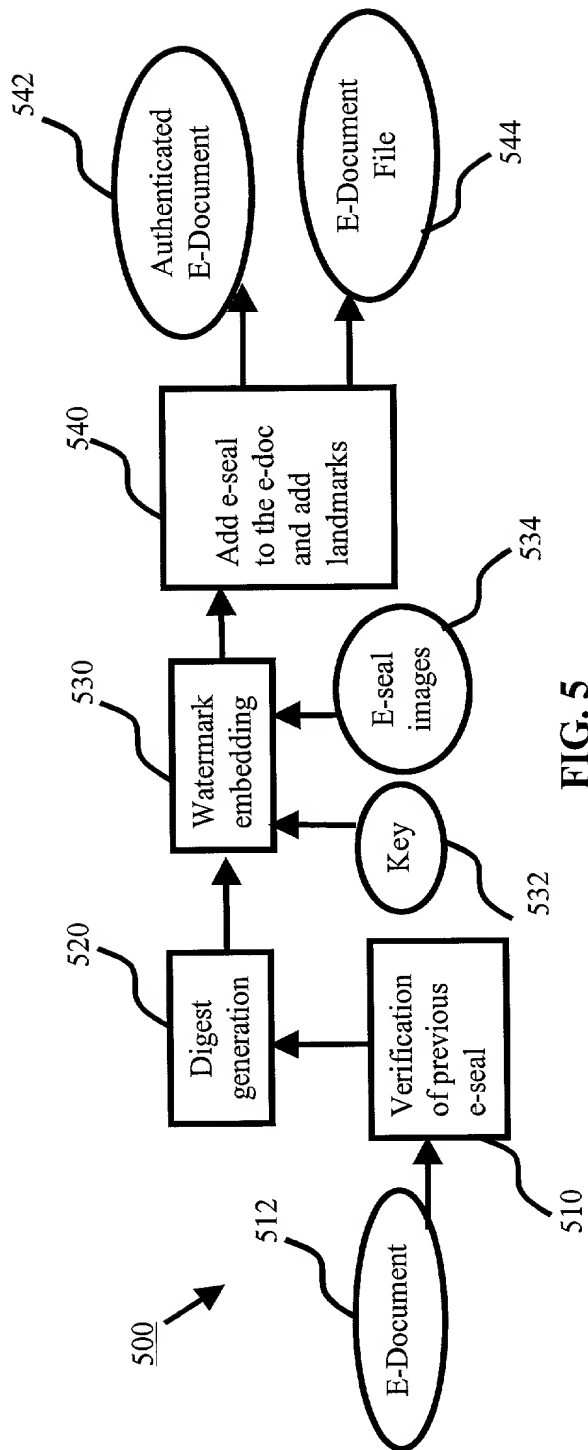
FIG. 3



420



FIG. 9



Please type a plus sign (+) inside this box → ☐

Docket No. 82231

PTO/SB/01 (12-97)

Approved for use through 9/30/00. OMB 0651-0032

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

**DECLARATION FOR UTILITY OR
DESIGN
PATENT APPLICATION
(37 CFR 1.63)**

☒ Declaration Submitted with Initial Filing **OR** ☐ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)

Attorney Docket Number

82231

First Named Inventor

WU, Jiankang

COMPLETE IF KNOWN

Application Number

/

Filing Date

Group Art Unit

Examiner Name

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Legitimacy Protection of Electronic Document and a Printed Copy Thereof

the specification of which

(Title of the Invention)

☐ is attached hereto
OR

☒ was filed on (MM/DD/YYYY)

08/21/1999

as United States Application Number or PCT International

Application Number **PCT/SG99/00086** and was amended on (MM/DD/YYYY) (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?	
				YES	NO
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto:

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below.

Application Number(s)	Filing Date (MM/DD/YYYY)	<input type="checkbox"/> Additional provisional application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

[Page 1 of 2]

Burden Hour Statement: This form is estimated to take 0.4 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Please type a plus sign (+) inside this box →



Approved for use through 9/30/00. OMB 0651-0032

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION — Utility or Design Patent Application

I hereby claim the benefit under 35 U.S.C. 120 of any United States application(s), or 365(c) of any PCT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. Parent Application or PCT Parent Number	Parent Filing Date (MM/DD/YYYY)	Parent Patent Number (if applicable)

☐ Additional U.S. or PCT international application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

As a named inventor, I hereby appoint the following registered practitioner(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

☐ Customer Number

OR

☐ Registered practitioner(s) name/registration number listed below

Place Customer
Number Bar Code
Label here

Name	Registration Number	Name	Registration Number

☐ Additional registered practitioner(s) named on supplemental Registered Practitioner Information sheet PTO/SB/02C attached hereto.

Direct all correspondence to: ☐ Customer Number or Bar Code Label ☐ OR ☐ Correspondence address below

Name					
Address					
Address					
City		State		ZIP	
Country		Telephone		Fax	

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name of Sole or First Inventor: ☐ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any])		Family Name or Surname	
<u>Jiankang</u>		<u>WU</u>	
Inventor's Signature			Date
			<u>5/2/00</u>
Residence: City	<u>Singapore</u>	State	Country
			<u>Singapore SGX</u>
Post Office Address	<u>Block 51, Teban Gardens Road, #06-565</u>		
Post Office Address			
City	<u>Singapore</u>	State	Country
			<u>Singapore</u>
		ZIP	<u>600051</u>

☒ Additional inventors are being named on the 1 supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto

Please type a plus sign (+) inside this box → +

Approved for use through 9/30/98. OMB 0651-0032

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION**ADDITIONAL INVENTOR(S)****Supplemental Sheet**Page 1 of 1**Name of Additional Joint Inventor, if any:**☐ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any])

Family Name or Surname

QibinSUNInventor's
Signature

Date

29/12/00

Residence: City

Singapore

State

Country

SGX
Singapore

Citizenship

China

Post Office Address

Block 52, Teban Gardens Road, #04-586

Post Office Address

City

Singapore

State

ZIP

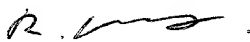
600052

Country

Singapore**Name of Additional Joint Inventor, if any:**☐ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any])

Family Name or Surname

HuijieDENGInventor's
Signature

Date

29/12/2000

Residence: City

Singapore

State

Country

SGX
Singapore

Citizenship

Singapore

Post Office Address

2 Namly Rise

Post Office Address

City

Singapore

State

ZIP

267110

Country

Singapore**Name of Additional Joint Inventor, if any:**☐ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any])

Family Name or Surname

Inventor's
Signature

Date

Residence: City

State

Country

Citizenship

Post Office Address

Post Office Address

City

State

ZIP

Country

Burden Hour Statement: This form is estimated to take 0.4 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Please type a plus sign (+) inside this box ➡ ☐

Docket No. 82231

PTO/SB/81 (11-96)

Approved for use through 6/30/99. OMB 0651-0035

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**POWER OF ATTORNEY OR
AUTHORIZATION OF AGENT,
NOT ACCOMPANYING
APPLICATION**

Application Number

Filing Date

First Named Inventor

WU, Jiankang

Group Art Unit

Examiner Name

Attorney Docket Number

I hereby appoint:

☐ Practitioners at Customer Number

OR

☒ Practitioner(s) named below:

Name	Registration Number
GARY M. NATH	26965
HAROLD L. NOVICK	26011

Place Customer
Number Bar Code
Label here

as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the Patent and Trademark Office connected therewith.

Please change the correspondence address for the above-identified application to:

☐ The above-mentioned Customer Number.

OR

☒ Firm or
Individual Name

NATH & ASSOCIATES

Address 1030 FIFTEENTH STREET, N.W.

Address SIXTH FLOOR

City WASHINGTON

State DC

ZIP 20005

Country U.S.A.

Telephone (202) 775 8383

Fax (202) 775 8396

I am the:

☒ Applicant.

☐ Assignee of record of the entire interest
Certificate under 37 CFR 3.73(b) is enclosed

SIGNATURE of Applicant or Assignee of Record

Name

WU, Jiankang

Signature

Date

29/02/00

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Please type a plus sign (+) inside this box➡

PTO/SB/81 (11-96)

Approved for use through 6/30/99. OMB 0651-0035

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays
a valid OMB control number.

**POWER OF ATTORNEY OR
AUTHORIZATION OF AGENT,
NOT ACCOMPANYING
APPLICATION**

Application Number	
Filing Date	
First Named Inventor	WU, Jiankang
Group Art Unit	
Examiner Name	
Attorney Docket Number	

I hereby appoint:

☐ Practitioners at Customer Number

OR

☒ Practitioner(s) named below:

*Place Customer
Number Bar Code
Label here*

Name	Registration Number
GARY M. NATH	26965
HAROLD L. NOVICK	26011

as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the Patent and Trademark Office connected therewith.

Please change the correspondence address for the above-identified application to:

☐ The above-mentioned Customer Number.

OR


<input checked="" type="checkbox"/> Firm or Individual Name	NATH & ASSOCIATES				
Address	1030 FIFTEENTH STREET, N.W.				
Address	SIXTH FLOOR				
City	WASHINGTON	State	DC	ZIP	20005
Country	U.S.A.				
Telephone	(202) 775 8383	Fax	(202) 775 8396		

I am the:

☒ Applicant.

☐ Assignee of record of the entire interest
Certificate under 37 CFR 3.73(b) is enclosed

SIGNATURE of Applicant or Assignee of Record

Name	SUN, Qibin
Signature	
Date	29/02/2000

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO:** Assistant Commissioner for Patents, Washington, DC 20231.

Please type a plus sign (+) inside this box ➡ ☐

Docket No. 82231

PTO/SB/81 (11-96)

Approved for use through 6/30/99. OMB 0651-0035

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**POWER OF ATTORNEY OR
AUTHORIZATION OF AGENT,
NOT ACCOMPANYING
APPLICATION**

Application Number

Filing Date

First Named Inventor

WU, Jiankang

Group Art Unit

Examiner Name

Attorney Docket Number

I hereby appoint:

☐ Practitioners at Customer Number

OR

☒ Practitioner(s) named below:

Name	Registration Number
GARY M. NATH	26965
HAROLD L. NOVICK	26011

Place Customer
Number Bar Code
Label here

as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the Patent and Trademark Office connected therewith.

Please change the correspondence address for the above-identified application to:

☐ The above-mentioned Customer Number.

OR

☒ Firm or
Individual Name

NATH & ASSOCIATES

Address

1030 FIFTEENTH STREET, N.W.

Address

SIXTH FLOOR

City

WASHINGTON

State

DC

ZIP

20005

Country

U.S.A.

Telephone

(202) 775 8383

Fax

(202) 775 8396

I am the:

☒ Applicant.

☐ Assignee of record of the entire interest

Certificate under 37 CFR 3.73(b) is enclosed

SIGNATURE of Applicant or Assignee of Record

Name

DENG, Huijie

Signature

H. Deng

Date

29/2/2000

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.